

**IN THE UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF TENNESSEE**

JOHN DOE,

Plaintiff,

v.

BELMONT UNIVERSITY,

Defendant.

)
)
)
)
)
)
)
)
)
)

Civil Action No. 3:17-cv-01245

Judge Waverly D. Crenshaw, Jr.

Mag. Judge Jeffrey S. Frensley

MEMORANDUM OF LAW REGARDING REMAINING DISCOVERY ISSUES

Pursuant to the judicial conference call held by phone on July 12, 2018, and Order of the Court filed that same day, the parties were directed to brief the remaining discovery issues by July 23, 2018. The remaining discovery issues, upon which the parties cannot reach an agreement are as follows:

- 1) Issues regarding the Family and Educational Rights and Privacy Act (Hereinafter (“FERPA”);
- 2) Requested social media platforms, logins and passwords;
- 3) Requested analysis of Plaintiff’s complete computer hard drive.

Each of these issues will be discussed in turn with legal support for each.

I. FERPA REGULATIONS

Plaintiff, in his discovery requests, has asked for several documents and files that are subject to FERPA regulations. Specifically, Plaintiff has requested:

- 1) Student S’s educational, disciplinary and/or conduct file, and transcript as requested in Document Request No. 1 and Supplementary Interrogatory Request No. 1-2;

- 2) All related documents, specifically disciplinary and/or conduct documents or records, for any Belmont students that have been suspended in the past 5 years, including the violation and their sex as stated in Interrogatory No. 9;
- 3) List all Belmont groups and clubs (or those associated with Belmont) that Student S. is a member of, or in which she participates;
- 4) Please also provide the disciplinary/conduct/educational records for these students designated as “Q, X, Y, and Z” in response to Interrogatory No. 16. We agree to the withholding of their names at the current time;
- 5) In regard to Interrogatory No. 19, who was the initial Belmont individual student S contacted regarding the Title IX accusation against Doe;
- 6) Additionally, in regard to Interrogatory No. 19, please provide a complete copy of the investigatory file (which should contain the information requested in).

All of the above, and presumably other issues and requests that are as yet unknown, deal with FERPA and the proper translation, understanding and application of the Act. It is very important for both sides to have this matter decided conclusively as it is either central or peripheral to most discovery in this case. In general, FERPA applies to all educational agencies receiving federal funding, including the case at bar. *Family educational and privacy rights*, 20 USCA § 1232g. FERPA, in addition to a number of other actions, protects educational records from disclosure without student and/or parent consent for such disclosure.¹ “No funds shall be made available under any applicable program to any educational agency or institution which has a policy

¹ FERPA applies to all educational institutions, therefore if a student is under 18 years of age his parents are the legal party.

or practice of permitting the release of education records (or personally identifiable information contained therein other than directory information, as defined in paragraph (5) of subsection (a)) of students without the written consent of their parents to any individual, agency, or organization, other than to the following--..." *Id.* It is the exceptions that are applicable in regard to the discovery requests in the case at bar. There are several exceptions listed, two of which are judicial order for release and a subpoena for release. *20 USCA §1232g b(2)B.*

In Title 34 of the Code of Federal Regulations (Hereinafter "CFR"), FERPA is further addressed, and is written in a manner that is perhaps easier to understand in regard to the nuances involved. Title 34, part 99 of the CFR states that an educational agency or institution may disclose personally identifiable information from an education record of a student without the consent required by § 99.30 if the disclosure meets one or more of several listed conditions. One such condition is:

(9)(i) The disclosure is to comply with ***a judicial order or lawfully issued subpoena***.(emphasis added).

(ii) The educational agency or institution may disclose information under paragraph (a)(9)(i) of this section only if the agency or institution makes a reasonable effort to notify the parent or eligible student of the order or subpoena in advance of compliance, so that the parent or eligible student may seek protective action, unless the disclosure is in compliance with—

(A) A Federal grand jury subpoena and the court has ordered that the existence or the contents of the subpoena or the information furnished in response to the subpoena not be disclosed;

(B) Any other subpoena issued for a law enforcement purpose and the court or other issuing agency has ordered that the existence or the contents of the subpoena or the information furnished in response to the subpoena not be disclosed; or

(C) An ex parte court order obtained by the United States Attorney General (or designee not lower than an Assistant Attorney General) concerning investigations or prosecutions of an offense listed in *18 U.S.C. 2332b(g)(5)(B)* or an act of domestic or international terrorism as defined in *18 U.S.C. 2331*.

Parts A, B and C above, serve only to illustrate the situations in which students would not be able to seek protective action regarding disclosure of their records. The records of a student can be disclosed with a court order or subpoena. The students does not need to *consent* to such release, when there is a subpoena or judicial order as they normally would. The educational institution need only make a reasonable effort to notify the student so they may seek protective action if they wish their records not be disclosed. It is important to repeat that *permission from the student is **not** required prior to disclosure*. The only requirement is that the student have an opportunity to object to the disclosure, however, the code is silent on how much time is required.

The Family Policy Compliance Office (Hereinafter “FPCO”)² of the Department of Education is the department tasked with overseeing FERPA. As a threshold matter, institutions should confirm that any subpoena received was, in fact, “lawfully issued.” This is simply a matter of confirming that the subpoena was issued in accordance with applicable state law. The institution next must make a “reasonable effort to notify” the student. This concept is not defined but the FCPO has offered guidance. In a February 16, 1999³ letter issued to Youngstown University, the agency advised that whether a university or college makes a reasonable attempt to notify a student in advance of complying with a subpoena is a “case-by-case” determination that takes into account “the totality of the circumstances.” The school should attempt to provide notice in a manner that

²See <https://www2.ed.gov/policy/gen/guid/fpc/index.html>

³ https://www2.ed.gov/policy/gen/guid/fpc/ferpa/library/youngstown_oh.html

is most likely to quickly reach the student. The FCPO acknowledged that FERPA does not define what constitutes a timely notice, but emphasized schools should strive to provide a sensible time period to allow a student to take action to quash a subpoena if they so desire. 20 USCA § 1232g does state a time period of 45 days, which was mentioned by opposing counsel in this regard. However, this 45 day time limit deals with the time period for granting a request by a parent for access to the education records of their children. The code states: “Each educational agency or institution shall establish appropriate procedures for the granting of a request by parents for access to the education records of their children within a reasonable period of time, but in no case more than forty-five days after the request has been made.” 20 USCA § 1232g. *Family educational and privacy rights*.

Thus, an institution *may* produce records in response to a lawfully issued subpoena or court order without the student’s consent, *after* it has made a reasonable effort to notify the student that it intends to do so. The institution is not required to obtain any consent or acknowledgement from the student in response. It is required only to provide the requisite notice. Therefore, since, on the whole, the only objection to the records Plaintiff requested was the restrictions of FERPA, Defendant should provide all documents requested by Plaintiff, as long as they meet the requirement that they are reasonably calculated to lead to the discovery of admissible evidence.

II. SOCIAL MEDIA

The Defendant requests, in their written discovery, identification and unlimited access to various social media platforms. It is requested that Plaintiff provide Defendant with his login and password for all active social media platforms. Defendant’s interrogatory No. 14 states: “Identify

each email service provider ...⁴ you used to communicate about any topics that concern any of your allegations in the Complaint or to communicated with any person (other than your attorneys) about any of the claims, facts, circumstances or allegations relating to or concerning your Complaint from the date you enrolled at Belmont to the present, and for each such site/service, provide:

- a. the full URL and/or the mobile application used to facilitate the communications;
- b. your use ID, screen name, user name, handle and any other identifier that associated the account with you; and
- c. all email addresses associated with your account.”

In response, Plaintiff made the relevant objections and stated that he did not use any social media sites to communicate the details of the case. Plaintiff stated under oath that he has not made any mention of his case, nor the facts surrounding his case on any social media platform. Therefore, the continued request for his social media usernames and passwords is inappropriate as it is irrelevant to the case and not calculated to lead to discoverable information.

In discussions with opposing counsel, my client has agreed to provide his entire facebook download with a protective order, to which opposing counsel has agreed, as a show of good faith and quite frankly because Plaintiff has nothing to hide and it is not worth the time and money spent arguing over a discovery issue that Plaintiff has no qualms about revealing. Plaintiff, however, is neither waiving his former objection nor his right to protect his privacy by this act of good faith and continues to contend the request is irrelevant according to his discovery answers.

⁴ all potential social media providers named here.

However, opposing counsel wants more, he wants unfettered access to all social media accounts. For my client to provide all other social media logins and passwords is unreasonable. There does not seem to be a manner in which my client could download all other platforms in the same manner as Facebook.⁵ Therefore, in order for Defendant to have access to the entire social media platform(s) and all postings, my client would have to provide the login and password for each site, which is unreasonable and not calculated to lead to discoverable information based on my client's response to the interrogatory, wherein he stated he did not use social media to communicate about the case.

While there is no guiding precedent from the Sixth Circuit, other courts have come to varying conclusions as to the discovery of information posted on social networking sites such as Facebook. While there are cases, though not in our district, that state Facebook information is discoverable because, according to these cases, the Facebook postings are not privileged and that their disclosure would not infringe upon a right of privacy, they are not relevant in the case at bar. *McMillen v. Hummingbird Speedway, Inc.*, 2010 Pa. Dist. & Cnty. Dec. LEXIS 270, 2010 WL 4403285 (Pa.Com.Pl. 2010), *Romano v. Steelcase, Inc.*, 30 Misc. 3d 426, 907 N.Y.S.2d 650 (2010). These cases rely on Fed.R.Civ.P. 26(b), which, as the Court is aware, states "[p]arties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense." Because my client has stated under oath that he did not use social media platforms whatsoever to discuss any details related to the case, the social media sites are neither relevant nor likely to lead to discoverable information. In *McCann v. Harleysville Ins. Co. of New York*, 78 AD3d 1524, 910 N.Y.S.2d 614 (N.Y. App.Div. 2010), the court upheld the denial of a motion to

⁵ If there is a manner, my client is still not obligated to provide the download based on his discovery responses.

compel Facebook information, not on grounds of privacy or privilege, but because the defendant "failed to establish a factual predicate with respect to the relevancy of the evidence," finding that "defendant essentially sought permission to conduct 'a fishing expedition' into plaintiff's Facebook account based on the mere hope of finding relevant evidence." *Id.* at 1525. That is exactly what Defendant is attempting to do in the case at bar and such unlimited access should not be granted. Defendant does not have a generalized right to rummage at will through information that Plaintiff has limited from public view. Rather, consistent with Rule 26(b), there must be a threshold showing that the requested information is reasonably calculated to lead to the discovery of admissible evidence. 20 USCA § 1232g Otherwise, the Defendant would be allowed to engage in the proverbial fishing expedition, in the hope that there might be something of relevance in one of Plaintiff's social media accounts.

Defendant has not made a sufficient predicate showing that the material it seeks is reasonably calculated to lead to the discovery of admissible evidence. *McCann, supra*, 78 A.D.3d at 1525. Moreover, the request for the entire account(s), which may well contain voluminous personal material having nothing to do with this case, is overly broad. "District courts have discretion to limit the scope of discovery where the information sought is overly broad or would prove unduly burdensome to produce." *Surles ex rel. Johnson v. Greyhound Lines, Inc.*, 474 F.3d 288, 305 (6th Cir.2007) (citing Fed.R.Civ.P. 26(b)(2)). Rule 26 "does not, however, permit a plaintiff to 'go fishing' and a trial court retains discretion to determine that a discovery request is too broad and oppressive."). For all of the foregoing reasons, Defendant is not entitled to Plaintiff's login(s) and Password(s) to his social media sites and the Facebook download is being given out of an abundance of good will.

III. PLAINTIFF'S COMPUTER

Defendants are requesting Plaintiff's entire computer. A computer in this day holds everything that has to do with being human; if you have a person's computer you can see into their soul- or at least their bank and library records. In all seriousness, with unfettered access to a person's hard drive, one will have access to personal notes, bank accounts, medical information, prescription information, information about friends and loved ones they have entrusted to us, addresses and phone numbers to all of our contacts, bank records, "to do" lists, novels and poetry we attempt but wish to keep private, personal and financial passwords to everything we are members of, information on our testing and job interview feedback, letters from significant others, any number of photographs and a host of other information.

Defendant does not have the right to "uncontrolled and unfettered disclosure" of Plaintiff's computer. *Gilman & Ciocia, Inc. v. Walsh*, 45 A.D.3d 531, 845 N.Y.S.2d 124 (2d Dept., 2007); Interpreting "material and necessary" liberally doesn't "mean that litigants have carte blanche to demand production of whatever ... they speculate might contain something hopeful." *Vyas v. Campbell*, 4 A.D.3d 417, 418, 771 N.Y.S.2d 375 [2d Dept., 2004]. "It is incumbent on the party seeking disclosure to demonstrate that the method of discovery sought will result in the disclosure of relevant evidence or is reasonably calculated to lead to the discovery of information bearing on the claims." *Id.* In the present case, Defendants have failed to do so and to allow them to seek for whatever they can find in Plaintiff's computer hard drive is not acceptable. If Defendants had a narrowed idea of the information they were seeking, the request would be more logical but this unfettered review of all Plaintiff's documents and private information is not what the Rules of Civil Procedure call for and should not be allowed." [C]ourts have been loath to sanction an

intrusive examination of an opponent's computer hard drive as a matter of course.” *Schreiber v. Schreiber*, 29 Misc.3d 171, 904 N.Y.S.2d 886 (Supreme Court Kings County 2010),

In most cases, the computer itself is not evidence. It is merely the instrument for creating evidence (like a typewriter) or the means of storing it (like a file cabinet). Increasingly, however, litigants have sought access to the opponent's computer or other electronic devices to search for evidence, especially for deleted e-mails. The federal courts have generally resisted such incursions. *Diepenhorst v. City of Battle Creek*, 2006 WL 1851243, at *2 (W.D.Mich.,2006)

The issues of concern are how to protect Plaintiff's confidential personal information that is stored on the computers, e.g., personal banking and credit card information, and how to prevent Plaintiff from waiving the attorney-client privilege by allowing the information on the computers to be viewed by any third party. Initially, the Court explains that the 2006 amendments to Rule 34 of the Federal Rules of Civil Procedure clarify “that discovery of electronically stored information stands on equal footing with discovery of paper documents.” Fed.R.Civ.P. 34 Advisory Committee's Note on 2006 Amendments. Consequently, without a qualifying reason, Defendants are no more entitled to access to Plaintiff's electronic information storage systems than to Plaintiff's warehouses storing paper documents. *See Scotts Co., LLC v. Liberty Mut. Ins. Co.*, No. 3:06-cv-899, 2007 U.S. Dist. LEXIS 43005, at *4-5 (S.D. Ohio June 12, 2007).

Thus, even if acceptable as a means to preserve electronic evidence, compelled forensic imaging is not appropriate in all cases, and courts must consider the significant interests implicated by forensic imaging before ordering such procedures. *Cf. Fed.R.Civ.P. 34(a)* Courts should guard against undue intrusiveness resulting from inspecting or testing electronic information systems.

The media at issue will almost certainly contain confidential state or private personal information that is wholly unrelated to the litigation. Although the risk of improperly exposing such information, standing alone, might not preclude the employment of forensic imaging in all cases, the forensic imaging must be premised on an interest significant enough to override that risk. *John B. v. Goetz*, 531 F.3d 448, 460–61 (C.A.6 (Tenn.),2008).

CONCLUSION

For the foregoing reasons Defendants should provide all information that is protected by FERPA as soon as possible to Plaintiff and Defendant should not be allowed unfettered access to Plaintiff's social media or computer hard drive.

Dated July 23, 2018.

/s/Michelle Owens
Michelle Owens BPBR No. 026512
Lynn Agee BPR No. 8448
Agee Owens & Cooper
2911 Elm Hill Pike
Nashville, TN 37027
(615) 300-8546
mowens@ageeowenslaw.com

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the forgoing was served via the Court's ECF filing system on the following:

Tim Palmer
Ogletree Deakins Nash Smoak & Stewart, P.C.
401 Commerce Street, Suite 1200
Nashville, TN 37219

on July 23, 2018.

s/Michelle Owens
Michelle Owens

